Confronting the new wave of cyberattacks

Email usage rose at 9 out of 10 companies, with 45% saying it was significant.

There's no doubt that cybercriminals have capitalised on the disruption caused over the past two years by the COVID-19 pandemic. The massive acceleration of digital transformation over this period has pushed cybersecurity to the top of the business agenda as the threat landscape has now been extended beyond the corporate walls to include the home office.

Attackers have been actively seeking weaknesses in remote systems and personal devices now being used for work purposes, while also exploiting the vulnerability of employees working from home.

In fact, hackers have ruthlessly taken advantage of the many negative psychological factors affecting employees' decision-making over this period, such as stress, uncertainty, anxiety and even distraction. Furthermore, the fact that many organisations have had to downscale on resources and ramp up cost cutting measures has led to employees taking on increasing workloads, making them more likely to let down their guard down for the sake of productivity and mistakenly click on a phishing link, for instance.

To this end, it is not surprising to learn that email security remains the top risk in cybersecurity, with over 90 percent of breaches occurring from various email related attacks. And, according to Gartner, business email compromise (BEC) attacks are expected to increase to over $5 billion by 2023.

This more remote workforce (be it temporary, permanent or a hybrid mix of the two) has confirmed the critical nature of end user awareness training in order to help employees to build healthier online habits, while also mitigating a business' exposure to cyberattacks, such as hacking and phishing scams.

Effective cybersecurity awareness training should therefore be adopted by all organisations as a proactive measure.

Users that are more cyber aware, making informed and safer decisions around email use, could be referred to as a 'human firewall', meaning that they are able to spot a suspicious character or document, and alert or notify the email administrator. In my opinion, this should then be rewarded by organisations, as while measuring the return on investment is sometimes challenging for businesses, the alternative is far worse.

In Mimecast sixth annual State of Email Security Report 2022 IT decision-makers shed light on three main elements:

- The cybersecurity challenges they continue to face such as phishing and ransomware
- The gains in cyber resilience that can come via new technology implementations
- External forces that impact their businesses such as budget increases or government mandates.

READ FULL REPORT >>